Amendments to the Specification:

Please **REPLACE** the paragraph beginning at page 3, line 22, with the following:

Hopefully, as soon as encryption is switched on, a fraudulent unit is immediately disclosed. This is because any such unit should not be in possession of the secret link key that is used by the devices originally involved in the link. Therefore, the unit is also unable to derive the encryption key. To further increase difficulties for a malicious unit, the creation of the encryption key is dependant not only on the link key, but also on a number that is denoted "Authentication Ciphering Offset" (ACO). The ACO is a number that is created for every call of the function that generates the SRES. If two units switch on encryption with different ACOs, their respective generated encryption key will differ even if they use the same link key. More information regarding the use of ACOs may be found in Section 3.2.2 of "Specification of the Bluetooth System, Version 1.2, Core System Package, Part H, November 2003".